On the key equation for n-dimensional cyclic codes. Applications to decoding

Hervé Chabanne, Graham H. Norton

INRIA

UNITÉ DE RECHERCHE
INRIA-ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tél. (1) 39 63 55 11

Rapports de Recherche

1992

25ème anniversaire

N° 1796

Programme 2
Calcul Symbolique, Programmation
et Génie logiciel

ON THE KEY EQUATION FOR *n*-DIMENSIONAL CYCLIC CODES. APPLICATIONS TO DECODING.

Hervé CHABANNE
Graham H. NORTON

Novembre 1992

RR_1796

On the key equation for n-dimensional cyclic codes. Applications to decoding.

—

Hervé CHABANNE
INRIA
projet CODES
Domaine de Voluceau, Rocquencourt, B.P. 105
78153 Le Chesnay Cedex
FRANCE

—

Graham H. NORTON (*)
Centre for Communications Research
Faculty of Engineering
University of Bristol
Bristol BS8 1TR
UNITED KINGDOM

(*) Research supported by Science and Engineering Research Council grant GR/H15141.

—

November 4, 1992

On the key equation for n-dimensional cyclic codes. Applications to decoding.

Sur l'équation clé d'un code multicyclique. Applications au décodage.

Hervé CHABANNE [1] Graham H. NORTON [2]

Abstract. We introduce the key equation of a multidimensional code. This equation exhibits the error-locator polynomial as product of univariate polynomials and the error-evaluator polynomial as a multivariate polynomial.

Then we reinterpret these polynomials in a multidimensional linear recurring sequence context. In particular, using the concept of section [8], we reduce the solution of the decoding problem to a succession of application of the Berlekamp-Massey algorithm.

However, it must be noted that multidimensional codes which are usefull for applications and which are decodable by our algorithm are left to be found.

Résumé. Nous introduisons l'équation clé d'un code multidimensionel. Cette équation fait intervenir le polynôme localisateur comme un produit de polynômes en une indéterminée et le polynôme évaluateur comme un polynôme en plusieurs indéterminées.

Ensuite nous réinterprétons ces polynômes dans un contexte de suites récurrentes linéaires multidimensionelles. En particulier, nous servant du concept de section [8], nous donnons une solution au problème du décodage en le réduisant à des utilisations successives de l'algorithme de Berlekamp-Massey.

Néanmoins, il faut noter que des codes multidimensionels ayant une utilité pratique et pouvant être décodés par notre algorithme restent à trouver.

[1]INRIA, projet CODES, Domaine de Voluceau, Rocquencourt, B.P. 105 78153 Le Chesnay Cedex, FRANCE.

[2]Centre for Communications Research, Faculty of Engineering, University of Bristol, Bristol BS8 1TR UNITED KINGDOM (Research supported by Science and Engineering Research Council grant GR/H15141).

1 Introduction and notation.

Let $R = K[X_1, ..., X_n]/(X_1^{N_1} - 1, ..., X_n^{N_n} - 1)$ be a multivariate residue class ring over a finite field K whose characteristic does not divide $N_1...N_n$.

Ideals in R are known as n-dimensional cyclic codes or abelian codes [1]-[3].

Let F be the smallest extension of K containing an N_v^{th} primitive root of unity α_v for $v = 1, ..., n$.

Let $e = e(X_1, ..., X_n) \in \mathsf{F}[X_1, ..., X_n]$ be a non-zero polynomial.

We consider the series

$$\Gamma_{\tilde{e}}(X_1^{-1}, ..., X_n^{-1}) = \sum_{i_1 \leq 0} ... \sum_{i_n \leq 0} e(\alpha_1^{-i_1}, ..., \alpha_v^{-i_n}) X_1^{i_1} ... X_n^{i_n} \in \mathsf{F}[[X_1^{-1}, ..., X_n^{-1}]].$$

We first introduce univariate polynomials $\sigma_v \in \mathsf{F}[X_v]$, $\sigma_v(X_v) | (X_v^{N_v} - 1)$, $v = 1, ..., n$ and a multivariate polynomial $\omega \in \mathsf{F}[X_1, ..., X_n]$ such that

$$\begin{cases} \sigma_1(X_1)...\sigma_n(X_n)\Gamma_{\tilde{e}}(X_1^{-1}, ..., X_n^{-1}) &= X_1...X_n\omega(X_1, ..., X_n) \\ gcd(\omega, \sigma_1...\sigma_n) &= 1 \end{cases}$$

Thus, we show that the spectral behaviour of $\sigma = \sigma_1...\sigma_n$ and ω allows us to recover e.

In the second part, we reinterpret the polynomials σ and ω, regarding $\Gamma_{\tilde{e}}$ as the generating function of the n-dimensional linear recurring sequence

$$\tilde{e} = \left(e(\alpha_1^{-i_1}, ..., \alpha_n^{-i_n})\right)_{i_1 \leq 0, ..., i_n \leq 0}.$$

In this manner, we show how to obtain σ_v, $v = 1, ..., n$ from partial knowledge of $\tilde{e}$.

Hence, applying our previous results, we deduce a new method for decoding n-dimensional cyclic codes [2], [10]. We give one example in the case $n = 2$ for an easier understanding. A different approach to decoding $2D$ cyclic codes is given in [10].

Notation

n	:=	Strictly positive integer
$[1,n]$	:=	$\{1,2,...,n\}$.
$\mathbf{X}$	:=	$X_1X_2...X_n$.
$\mathbf{0}$	:=	(0,...,0).
$\mathbf{1}$	:=	(1,...,1).
α_v	:=	primitive N_v^{th} root of 1, $v \in [1,n]$
$\mathsf{F}[\mathbf{X}]$	:=	$\mathsf{F}[X_1, X_2, ..., X_n]$.
$\mathsf{F}((\mathbf{X^{-1}}))$	:=	Laurent series in $\mathbf{X^{-1}}$ over F.
$\mathsf{F}[\widehat{X_v}]$	:=	$\mathsf{F}[X_1, X_2, ..., X_{v-1}, X_{v+1}, ..., X_n]$.
$\widehat{X_v}$	:=	$X_1X_2...X_{v-1}X_{v+1}...X_n := \mathbf{X}/X_v$.
$\mathbf{i}$	:=	$(i_1, i_2, ..., i_n)$.
$\mathbf{X^i}$	:=	$X_1^{i_1}X_2^{i_2}...X_n^{i_n}$.
$\pi_v(\mathbf{i})$	:=	i_v.
$\widehat{\pi_v}(\mathbf{i})$	:=	$(i_1, ..., i_{v-1}, i_{v+1}, ..., i_n)$
$\mathbf{i} \preceq \mathbf{k}$	$\Leftrightarrow$	$i_v \leq k_v,\ v \in [1,n]$.
$supp(\sum_{\mathbf{i}} p_{\mathbf{i}}\mathbf{X^i})$	:=	$\{\mathbf{i} : p_{\mathbf{i}} \neq 0 \in \mathsf{F}\}$.
$\delta_v(p)$	:=	The degree of $p \in \mathsf{F}[\mathbf{X}]$ considered as a polynomial in $\mathsf{F}[X_v]$.
$\delta(p)$	:=	$(\delta_1(p), ..., \delta_n(p))$

2 The key equation.

Let $e(\mathbf{X}) = \sum_{\mathbf{i} \in supp(e)} e_{\mathbf{i}} \mathbf{X}^{\mathbf{i}} \in \mathsf{F}[\mathbf{X}]$ be a non-zero polynomial. We abbreviate $e(\alpha_1^{i_1}, ..., \alpha_n^{i_n})$ to $e(\alpha^{\mathbf{i}})$. Our goal is to show how the series $\Gamma_e = \Gamma_e(\mathbf{X}^{-1}) = \sum_{\mathbf{i} \preceq \mathbf{0}} e(\alpha^{-\mathbf{i}}) \mathbf{X}^{\mathbf{i}} \in \mathsf{F}[[\mathbf{X}^{-1}]]$ may be written as a quotient of two relatively prime polynomials.

Following Pedersen [9], we introduce the set of *grid-points* of e, $\Xi_e = \bigcap_{v=1}^{n} \pi_v^{-1}(\pi_v(supp(e))) = \{\mathbf{i} \in \mathsf{N}^n \ : \ i_v \in \pi_v(supp(e)), v \in [1,n]\}$. Clearly Ξ_e is the smallest cartesian product which contains $supp(e)$.

We begin by recalling a simple lemma, which is easily proved by induction on n.

Lemma 1 *For $v \in [1,n]$ and $\beta_v \in \mathsf{F}((X_v^{-1}))$, $\sum_{\mathbf{i} \succeq \mathbf{0}} \beta_1^{i_1} \beta_2^{i_2} ... \beta_n^{i_n} = \prod_{v=1}^{n} (1 - \beta_v)^{-1}$*

Proof : Omitted. □

Proposition 1 $\Gamma_e = \sum_{\mathbf{i} \in supp(e)} \frac{e_{\mathbf{i}}}{\prod_{v=1}^{n} (1 - \alpha_v^{i_v} X_v^{-1})}$.

Proof : $\Gamma_e = \sum_{\mathbf{j} \succeq \mathbf{0}} e(\alpha^{\mathbf{j}}) \mathbf{X}^{-\mathbf{j}} = \sum_{\mathbf{j} \succeq \mathbf{0}} \left(\sum_{\mathbf{i} \in supp(e)} e_{\mathbf{i}} (\alpha^{\mathbf{j}})^{\mathbf{i}} \right) \mathbf{X}^{-\mathbf{j}}$

$= \sum_{\mathbf{i} \in supp(e)} e_{\mathbf{i}} \left(\sum_{\mathbf{j} \succeq \mathbf{0}} (\alpha^{\mathbf{i}} \mathbf{X}^{-1})^{\mathbf{j}} \right) = \sum_{\mathbf{i} \in supp(e)} \frac{e_{\mathbf{i}}}{\prod_{v=1}^{n} (1 - \alpha_v^{i_v} X_v^{-1})}$ by the lemma. □

We can now introduce n-dimensional analogues of the error-locator and error-evaluator polynomials.

Definition 1 *For $v \in [1,n]$, define the error-locator X_v-polynomial $\sigma_v \in \mathsf{F}[X_v]$ by*

$$\sigma_v = \sigma_v(X_v) = \prod_{i_v \in \pi_v(supp(e))} (X_v - \alpha_v^{i_v})$$

We call $\sigma = \sigma(\mathbf{X}) = \prod_{v=1}^{n} \sigma_v(X_v)$ the error-locator product polynomial of e.

Finally, we call

$$\omega = \omega(\mathbf{X}) = \sum_{\mathbf{i} \in supp(e)} e_{\mathbf{i}} \left(\prod_{v=1}^{n} \prod_{\substack{j \in \pi_v(supp(e)) \\ j \neq i_v}} (X_v - \alpha_v^j) \right)$$

the error-evaluator polynomial of e.

We note that, as in the one-dimensional case,

$$\sigma'_v(X_v) = \sum_{i_v \in \pi_v(supp(e))} \prod_{\substack{j \in \pi_v(supp(e)) \\ j \neq i_v}} (X_v - \alpha_v^j)$$

and

$$\sigma'_v(\alpha_v^{i_v}) = \prod_{\substack{j \in \pi_v(supp(e)) \\ j \neq i_v}} (\alpha_v^{i_v} - \alpha_v^j) \neq 0, \ \textit{if } \mathbf{i} \in supp(e).$$

Also $\delta_v \sigma = \delta_v \sigma_v = |\pi_v(supp(e))|$, $\delta\omega = \delta\sigma - 1$ and σ is monic.

Our reason for calling ω the error evaluator polynomial of e will become clear from Proposition 2 below. We are now ready to state the key equation.

Theorem 1 *In* $\mathsf{F}((\mathbf{X}^{-1}))$, *we have*

$$\sigma\Gamma_{\hat{e}} = \mathbf{X}\omega.$$

Proof : From Proposition 1, we have

$$\sigma(\mathbf{X})\Gamma_{\hat{e}} = \sum_{\mathbf{i} \in supp(e)} \frac{e_{\mathbf{i}}\sigma(\mathbf{X})}{\prod_{v=1}^{n}(1 - \alpha_v^{i_v} X_v^{-1})}$$

$$= \sum_{\mathbf{i} \in supp(e)} e_{\mathbf{i}} \left[\prod_{v=1}^{n} \prod_{i_v \in \pi_v(supp(e))} (X_v - \alpha_v^{i_v})\right] \left[\prod_{v=1}^{n} \frac{X_v}{X_v - \alpha_v^{i_v}}\right]$$

$$= \mathbf{X} \sum_{\mathbf{i} \in supp(e)} e_{\mathbf{i}} \left[\prod_{v=1}^{n} \prod_{\substack{j \in \pi_v(supp(e)) \\ j \neq i_v}} (X_v - \alpha_v^j)\right] = \mathbf{X}\omega(\mathbf{X}). \qquad \square$$

The spectral behaviour of ω in the next result justifies our use of the term " error evaluator polynomial " :

Proposition 2

$$\begin{aligned} \omega(\alpha^{\mathbf{i}}) &= e_{\mathbf{i}} \prod_{v \in [1,n]} \sigma'_v(\alpha_v^{i_v}) \neq 0 \quad \textit{if } \mathbf{i} \in supp(e) \\ &= 0 \qquad\qquad\qquad\qquad \textit{if } \mathbf{i} \in \Xi_e \setminus supp(e) \end{aligned}$$

Proof : If $\mathbf{i} \in supp(e)$, then

$$\omega(\alpha^{\mathbf{i}}) = e_{\mathbf{i}} \prod_{v=1}^{n} \prod_{\substack{l \in \pi_v(supp(e)) \\ l \neq i_v}} (\alpha_v^{i_v} - \alpha_v^l)$$

$$+ \sum_{\substack{\mathbf{k} \in supp(e) \\ \mathbf{k} \neq \mathbf{i}}} e_{\mathbf{k}} \prod_{v=1}^{n} \prod_{\substack{l \in \pi_v(supp(e)) \\ l \neq k_v}} (\alpha_v^{i_v} - \alpha_v^l)$$

$= e_{\mathbf{i}} \prod_{v \in [1,n]} \sigma_v'(\alpha_v^{i_v}) \neq 0$ since we may choose a v so that all other products cancel.

If $\mathbf{i} \in \Xi_e \backslash supp(e)$, then $\mathbf{i} \succeq \mathbf{0}$ and $i_v \in \pi_v(supp(e))$ for all $v \in [1,n]$, but for all $\mathbf{j} \in supp(e)$ there is a $v \in [1,n]$ with $i_v \neq j_v$. Therefore

$$\omega(\alpha^{\mathbf{i}}) = \sum_{\mathbf{j} \in supp(e)} e_{\mathbf{j}} \prod_{v=1}^{n} \prod_{\substack{l \in \pi_v(supp(e)) \\ l \neq j_v}} (\alpha_v^{i_v} - \alpha_v^l) = 0$$

since we may take $l = i_v$ in the product. □

Remark : We can see Theorem 1 as generalization of the key equation for BCH codes to n-dimensional cyclic codes. As for the cyclic case, the spectral behaviour of ω and σ allow us to recover e with Proposition 2 and

$$\begin{aligned} \sigma(\alpha^{\mathbf{i}}) &= e_{\mathbf{i}} \prod_{v \in [1,n]} \sigma_v'(\alpha_v^{i_v}) \neq 0 \quad if\ \mathbf{i} \notin \Xi_e \\ &= 0 \qquad\qquad\qquad\qquad\quad if\ \mathbf{i} \in \Xi_e \end{aligned}$$

□

We conclude this section by showing that σ and ω are relatively prime.

Corollary 1

$$gcd(\sigma, \omega) = 1$$

Proof : Since σ is a product of factors $X_v - \alpha_v^l$ for $l \in \pi_v(supp(e))$, $(\sigma, \omega) \neq 1$ implies that a factor $X_v - \alpha_v^l$ divides ω. In particular, if $\mathbf{i} \in supp(e)$ and $i_v = l$, then $\omega(\alpha^{\mathbf{i}}) = 0$, which contradicts Proposition 2. □

3 The linear recurring sequence context.

In this section, we reinterpret the polynomials σ and ω, regarding $\Gamma_{\tilde{e}}$ as the generating function of an n-dimensional linear recurring sequence $\tilde{e}$.

As in [8], we let $S^n_{\preceq \mathbf{0}}(\mathsf{F})$ denote the commutative F-algebra of $(-\mathbb{N})^n$-indexed sequences $s : (-\mathbb{N})^n \to \mathsf{F}$.

The action of $f \in \mathsf{F}[\mathbf{X}]$ on $s \in S^n_{\preceq \mathbf{0}}(\mathsf{F})$ given by

$$(f \circ s)_{\mathbf{j}} = \left((\sum_{\mathbf{i} \in supp(f)} f_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}) \circ s \right)_{\mathbf{j}} = \sum_{\mathbf{i} \in supp(f)} f_{\mathbf{i}} s_{\mathbf{j}-\mathbf{i}},$$

where $\mathbf{j} \preceq \mathbf{0}$, (i.e. via *right* shifting) makes $S^n_{\preceq \mathbf{0}}(\mathsf{F})$ into $\mathsf{F}[\mathbf{X}]$ module. The generating function of s is $\Gamma_s(\mathbf{X}^{-1}) = \sum_{\mathbf{i} \preceq 0} s_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$.

Definition 2 *If* $s \in S^n_{\preceq \mathbf{0}}(\mathsf{F})$, $Ann(s) = \{f \in \mathsf{F}[\mathbf{X}] \ : \ f \circ s = 0\}$ *is called the* characteristic ideal *of* s.

We say that s is a linear recurring sequence if $Ann(s)$ contains a non-zero (*characteristic*) polynomial. Recall that a sequence s is n-periodic if $X_v^{p_v} - 1 \in Ann(s)$, $p_v > 0$ and $v \in [1, n]$. In section 2 we studied the sequence $\tilde{e} \in S^n_{\preceq \mathbf{0}}(\mathsf{F})$ given by $\tilde{e}_{\mathbf{i}} = e(\alpha^{-\mathbf{i}})$, where $e \in \mathsf{F}[\mathbf{X}]$ is non-zero.

Proposition 3 *$\tilde{e}$ is n-periodic.*

Proof : This is a simple consequence of the fact that α_v is an N_v^{th} root of unity, $v \in [1, n]$. □

In particular, $\tilde{e}$ is a linear recurring sequence.

Definition 3 *[8] We say that a linear recurring sequence* $s \in S^n_{\preceq \mathbf{0}}(\mathsf{F})$ *is* ultimately rectilinear *if for all* $v \in [1, n]$, $Ann(s) \bigcap \mathsf{F}[X_v]$ *contains a polynomial of positive degree. If* s *is ultimately rectilinear, the monic positive of minimal (positive) degree in* $Ann(s) \bigcap \mathsf{F}[X_v]$ *is called the* minimal X_v-polynomial *of* s, *written* $\mu_v(s)$, *or* μ_v *if* s *is understood.*

Clearly $\tilde{e}$ is ultimately rectilinear. Our goal is to show that $\mu_v(\tilde{e}) = \sigma_v$, $v \in [1, n]$.

Proposition 4

$$f \in Ann(s) \Leftrightarrow \forall \mathbf{i} \in (-\mathbb{N})^n, coeff(\mathbf{X}^{\mathbf{i}}, f\Gamma_s) = 0.$$

Proof : Let $f(\mathbf{X}) = \sum_{\mathbf{j} \in supp(f)} f_{\mathbf{j}} \mathbf{X}^{\mathbf{j}}$. Then $coeff(\mathbf{X}^{\mathbf{i}}, f\Gamma_s) = \sum_{\mathbf{j} \in supp(f)} f_{\mathbf{j}} s_{\mathbf{i}-\mathbf{j}} = (f \circ s)_{\mathbf{i}}$ □

Proposition 5 *Let* $s \in S^n_{\preceq \mathbf{0}}(\mathsf{F})$ *be ultimately rectilinear and* $f_v \in Ann(s) \bigcap \mathsf{F}[X_v]$, $\delta_v f_v \geq 1$, $v \in [1, n]$. *Then* $\mathbf{X}^{-\mathbf{1}}(\prod_{v=1}^{n} f_v)\Gamma_s \in \mathsf{F}[\mathbf{X}]$.

Proof : Let $p = (\prod_{v=1}^{n} f_v)\Gamma_s \in \mathsf{F}((\mathbf{X}^{-1}))$. For $i \leq 0$, we have $coeff(X_v^i, p) = coeff(X_v^i, f_v\Gamma_s) = 0$ by Proposition 4. This is true for $v \in [1,n]$, so $p \in \mathsf{F}[\mathbf{X}]$ and $\mathbf{X}$ divides p. □

If s is ultimately rectilinear and $f_v \in Ann(s) \bigcap \mathsf{F}[X_v]$, $\delta_v f_v \geq 1$, $v \in [1,n]$, we will write $(\prod_{v=1}^{n} f_v)\Gamma_s = \mathbf{X}p(\prod_{v=1}^{n} f_v, s)$, where $p(\prod_{v=1}^{n} f_v, s)$ is a well-defined *polynomial* in $\mathbf{X}$.

For $v \in [1,n]$, there is a sequence $s^{(v)} \in S^1_{\leq 0}(\mathsf{F}[[\widehat{X_v}]])$ given by $s^{(v)}_{\mathbf{i}} = \sum_{\mathbf{j} \in (-\mathsf{N})^{n-1}} s_{\mathbf{i},\mathbf{j}} \widehat{X_v}^{\mathbf{j}}$, where $\mathbf{i}, \mathbf{j} \in (-\mathsf{N})^n$ denotes the index which projects onto $\mathbf{i}$ and onto $\mathbf{j}$ ($\widehat{\pi_v}(\mathbf{i}, j) = \mathbf{i}$, $\pi_v(\mathbf{i}, j) = j$).

Lemma 2

$$Ann(s^{(v)}) = Ann(s) \bigcap \mathsf{F}[X_v].$$

Proof : Let $f_v \in \mathsf{F}[X_v]$. A simple verification shows that $\Gamma_{f_v o s^{(v)}}(X_v^{-1}) = \Gamma_{f_v o s}(\mathbf{X}^{-\mathbf{i}})$, whence the result. □

Theorem 2 *For $v \in [1,n]$, $\sigma_v = \mu_v(\tilde{e})$.*

Proof : From the previous lemma, σ_v, $\mu_v \in Ann(\tilde{e}^{(v)})$ and $\delta_v \mu_v$ is the minimal degree in $Ann(\tilde{e}^{(v)})$; otherwise μ_v cannot be the minimal X_v-polynomial of $\tilde{e}$. Thus $\delta_v \mu_v \leq \delta_v \sigma_v$.

On the other hand,

$$\frac{\mathbf{X}\omega}{\prod_{v=1}^{n} \sigma_v} = \Gamma_{\tilde{e}} = \frac{\mathbf{X}p(\prod_{v=1}^{n} \mu_v, \tilde{e})}{\prod_{v=1}^{n} \mu_v}$$

and so $(\prod_{v=1}^{n} \mu_v)\omega = (\prod_{v=1}^{n} \sigma_v)p(\prod_{v=1}^{n} \mu_v, \tilde{e})$. Now σ and ω are relatively prime (Corollary 1) and so σ_v divides μ_v. Since $\delta_v \mu_v \leq \delta_v \sigma_v$ and μ_v is monic, we must have $\mu_v = \sigma_v$. □

We conclude this section by recalling how μ_v, the minimal X_v-polynomial of $\tilde{e}$, may be computed. First, we need to define the sections of a sequence.

Definition 4 *[8] Let $n \geq 2$ and let $v \in [1,n]$. For $\mathbf{i} \in (-\mathsf{N})^{n-1}$ define the $\mathbf{i}$-section of s, $s^{\S(v)}_{\mathbf{i}} \in S^1_{\leq 0}(\mathsf{F})$ by*

$$(s^{\S(v)}_{\mathbf{i}})_j = s_{\mathbf{k}} \ , \ j \in -\mathsf{N}$$

where $\widehat{\pi_v}(\mathbf{k}) = \mathbf{i}$ and $\pi_v(\mathbf{k}) = j$.

Notice that each $Ann(s^{\S(v)}_{\mathbf{i}})$ is principal ideal.

Lemma 3 *1.* $Ann(s)\bigcap \mathsf{F}[X_v] = \bigcap_{\mathbf{i}\in(-\mathbf{N})^{n-1}} Ann(s_{\mathbf{i}}^{\S(v)})$.

2. If $f_v \in Ann(s)\bigcap \mathsf{F}[X_v]$, $\delta_v f_v \geq 1$, $v \in [1,n]$. *Put* $\mathbf{d_v} = \delta(\prod_{u=1,u\neq v}^{n} f_u)$. *Then*

$$\bigcap_{\mathbf{i}\in(-\mathbf{N})^{n-1}} Ann(s_{\mathbf{i}}^{\S(v)}) = \bigcap_{\mathbf{0}\preceq\mathbf{i}\preceq\mathbf{d_v}-\mathbf{1}} Ann(s_{\mathbf{i}}^{\S(v)}).$$

Proof :

1. Let $g \in \mathsf{F}[X_v]$ and $j \in -\mathbf{N}$. Then

$$(g \circ s_{\mathbf{i}}^{\S(v)})_j = \sum_{k=0}^{\delta_v g} g_k (s_{\mathbf{i}}^{\S(v)})_{j-k} = \sum_{k=0}^{\delta_v g} g_k s_{j-k,\mathbf{i}} = (g \circ s)_{j,\mathbf{i}}.$$

   Thus $g \in Ann(s_{\mathbf{i}}^{\S(v)})$ for all $\mathbf{i}$ if and only if $(g \circ s_{\mathbf{i}}^{\S(v)})_j = 0$ for all $\mathbf{i}, j$ if and only if $g \in Ann(s)$.

2. It suffices to show that if $g \in \mathsf{F}[X_v]$ satisfies $g \circ s_{\mathbf{i}}^{\S(v)}$ for $0 \preceq \mathbf{i} \preceq \mathbf{d_v}$, then $g \circ s_{\mathbf{i}}^{\S(v)} = 0$ for all $\mathbf{i}$. Let $v = 1$ and $j \in -\mathbf{N}$. Without loss of generality, we can assume that each f_u is monic, $u \in [1,n]$. Suppose first that $\mathbf{i} = (\delta_2 f_2, \delta_3 f_3 - 1, ..., \delta_n f_n - 1)$. Since $f_2 \in Ann(s)$,

$$0 = (f_2 \circ s)_{j-k,\mathbf{i}} = \sum_{l=0}^{\delta_2 f_2} (f_2)_l s_{j-k,l,\mathbf{i}'},$$

   where $\mathbf{i}' = (\delta_3 f_3 - 1, ..., \delta_n f_n - 1)$ and so $s_{j-k,\mathbf{i}} = -\sum_{l=0}^{\delta_2 f_2} (f_2)_l s_{j-k,l,\mathbf{i}'}$. Now

$$(g\circ s_{\mathbf{i}}^{\S(v)})_j = (g\circ s)_{j,\mathbf{i}} = \sum_{k=0}^{\delta g} g_k s_{j-k,\mathbf{i}} = -\sum_{l=0}^{\delta_2 f_2} (f_2)_l \left(\sum_{k=0}^{\delta g} g_k s_{j-k,l,\mathbf{i}'}\right) = -\sum_{l=0}^{\delta_2 f_2} (f_2)_l (g\circ s_{l,\mathbf{i}'}^{\S(v)})_j = 0$$

   since $0 \preceq l, \mathbf{i}' \preceq \mathbf{d_1} - 1$. Thus for $\mathbf{i} = (\delta_2 f_2, \delta_3 f_3 - 1, ..., \delta_n f_n - 1)$, $g \circ s_{\mathbf{i}}^{\S(v)} = 0$. The argument is similar for $\mathbf{i} = (i_2, \delta_3 f_3 - 1, ..., \delta_n f_n - 1)$, $i_2 > \delta_2 f_2$. Suppose inductively that the result is true for $(i_2, ..., i_{k-1}, \delta_k f_k, ..., \delta_n f_n - 1)$ and $\mathbf{i} = (i_2, ..., i_k, \delta_{k+1} f_{k+1} - 1, ..., \delta_n f_n - 1)$, $i_k \geq \delta f_k$. An analogous argument also shows that $g \circ s_{\mathbf{i}}^{\S(v)} = 0$ by induction for all $\mathbf{i}$. It is clear that the same argument applies to any v, $1 \leq v \leq n$ and this completes the proof.

□

Theorem 3 *Let* $f_v \in Ann(\tilde{e})\bigcap \mathsf{F}[X_v]$, $\delta_v f_v \geq 1$, *for* $v \in [1,n]$. *Put* $\mathbf{d_v} = \delta(\prod_{u=1,u\neq v}^{n} f_u)$. *Then*

$$\sigma_v = lcm\{g_{\mathbf{i}} \ : \ (g_{\mathbf{i}}) = Ann(s_{\mathbf{i}}^{\S(v)}), \mathbf{0} \preceq \mathbf{i} \preceq \mathbf{d_v} - \mathbf{1}\}.$$

Proof : This follows immediately from Theorem 2 and Lemma 3 since each $Ann(s_i^{\S(v)})$ is principal, and their finite intersection is generated by their *lcm*. □

Remarks :

1. Once $\sigma_1, ..., \sigma_{n-1}$ have been computed, we can replace f_v by σ_v for $v \in [1, n-1]$, $n \geq 2$.
2. We have proved Theorem 2 without using the initial polynomial of σ and $\tilde{e}$

$$\iota(\sigma, \tilde{e}) = \sum_{i=0}^{\delta\sigma-1} \left(\sum_{j=i+1}^{\delta\sigma} \sigma_j \tilde{e}_{i-j+1} \right) \mathbf{X}^i$$

as defined in [8]. Of course, $p(\prod_{v=1}^{n} \mu_v, \tilde{e}) = \iota(\prod_{v=1}^{n} \mu_v, \tilde{e})$ and it follows that $\omega = \iota(\prod_{v=1}^{n} \sigma_v, \tilde{e})$. Thus by [8] Theorem 6.2, 6.3, we know that $Ann(\tilde{e})$ is the ideal quotient $(\sum_{v=1}^{n}(\sigma_v) : \omega)$.

□

4 Decoding Algorithm.

In this section we propose an algorithmic solution to the following problem :

(A) Given a non-zero $e \in K[\mathbf{X}]$ *and " enough " terms of the series* $\Gamma_{\hat{e}}(\mathbf{X^{-1}})$, *find* $\omega, \sigma \in \mathsf{F}[\mathbf{X}]$ *such that*

$$\begin{cases} \Gamma_{\hat{e}}(\mathbf{X^{-1}}) & = & \dfrac{\mathbf{X}\omega(\mathbf{X})}{\sigma(\mathbf{X})} \\ gcd(\omega, \sigma) & = & 1 \\ \sigma \text{ monic.} \end{cases}$$

It is well known that when $n = 1$, this problem may be solved using the Berlekamp Massey algorithm or equivalently the extended Euclidean algorithm ; see [4] for example. If we know $d-1$ consecutive terms of $\Gamma_{\hat{e}}(\mathbf{X^{-1}})$, then we can solve *(A)* for unique ω and σ such that $\deg\omega \leq \tau - 1$, $\deg\sigma \leq \tau$, where $\tau = \left[\dfrac{d-1}{2}\right]$.

We illustrate by means of an example how to decode an abelian code [1].

Example :

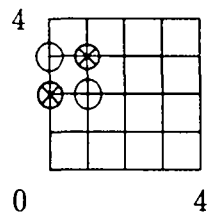
We take $K = GF(2)$, $N_1 = N_2 = 5$, $\alpha_1 = \alpha_2 = \alpha = \theta^3$ where $\theta^4 + \theta + 1 = 0 \in GF(2)$. Thus $\mathsf{F} = GF(16)$. Let C be the abelian code in $K[\mathbf{X}]/(X_1^5 - 1, X_2^5 - 1)$ defined by its non-zeroes $\{(1,1), (\alpha, \alpha^2), (\alpha^2, \alpha^4), (\alpha^4, \alpha^3), (\alpha^3, \alpha)\}$. It is a $[25, 5, 5]$ binary code [1].

Suppose we wish to decode the $e(\mathbf{X}) = X_2^2 + X_1 X_2^3$.

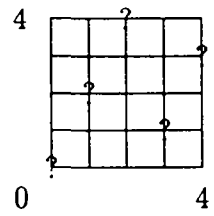
The values $e(\alpha^i, \alpha^j)$ are given by

j/i	0	1	2	3	4
4	$\alpha^2+\alpha^3$	0	$\alpha^3+\alpha^4$	$1+\alpha^3$	$\alpha+\alpha^3$
3	$\alpha+\alpha^4$	$1+\alpha$	0	$\alpha^2+\alpha$	$\alpha+\alpha^3$
2	$\alpha+\alpha^4$	$\alpha^2+\alpha^4$	$\alpha^3+\alpha^4$	0	$1+\alpha^4$
1	$\alpha^2+\alpha^3$	$\alpha^2+\alpha^4$	$1+\alpha^2$	$\alpha^2+\alpha$	0
0	0	$1+\alpha$	$1+\alpha^2$	$1+\alpha^3$	$1+\alpha^4$

We may represent the decoding problem graphically as



$\otimes$: $supp(e)$
$\Xi_e : \otimes \cup \bigcirc$



? : unknown position of $\Gamma_{\tilde{e}}(\mathbf{X}^{-1})$

We begin by decoding the first row. That is, we calculate the minimal X_1-polynomial of $\tilde{e}_0^{\S(1)}$ using the extended Euclidean algorithm.

We obtain $X_1^2 + (1+\alpha)X_1 + \alpha = (X_1+1)(X_1+\alpha)$.

The other rows are decoded in the same way ; decoding is always possible since for each row the numbers of errors may not exceed 2 and we know $d-1=4$ consecutive terms. We obtain the same minimal polynomial for each row, and by Theorem 3, $\sigma_1 = (X_1+1)(X_1+\alpha)$. We obtain the unknown positions in $\Gamma_{\tilde{e}}$ from these polynomials. Column by column decoding yields $\sigma_2(X_2) = X_2^2 + (\alpha^3+\alpha^2)X_2 + 1 = (X_2+\alpha^2)(X_2+\alpha^3)$.

Theorem 1 now implies that $\omega = \sigma\Gamma_{\tilde{e}}/\mathbf{X}$. We find $\omega(\mathbf{X}) = (\alpha^2+\alpha^4)+(\alpha^2+\alpha^3)X_1+(1+\alpha)X_2$. We have decoded correctly since ω vanishes on the positions ◯ but does not vanish on the positions ⊗. □

Remarks :

1. The errors $e(\mathbf{X}) + X_2^3$, $e(\mathbf{X}) + X_1X_2^2$ and $e(\mathbf{X}) + X_1X_2^2 + X_2^3$ can be decoded in the same way

2. In [10], the author defines an " error-locator ideal " I_e for certain $2D$ cyclic codes and decodes them by finding a Grœbner basis for I_e. For our example, this method requires that some values of $\tilde{e}$ are known. If these values are not known, some trials Grœbner bases of I_e have to be tested.

□

More generally we have

Algorithm 1

1. *From the known terms of* $\tilde{e}_i^{\S(v)}$ *find*
   - $g_i^{\S(v)}$ *such that* $(g_i^{\S(v)}) = Ann(\tilde{e}_i^{\S(v)})$ *(used in point 2),*
   - *the missing terms of* $\tilde{e}_i^{\S(v)}$ *(used in point 3).*

   (In order to perform this task, one can use the Euclidean extended algorithm, the Berlekamp Massey algorithm with or without erasures [2] or try each factor of $X_v^{N_v} - 1$ *in turn. If no algorithm is available, put* $g_i^{\S(v)} = 1$ *for convenience.)*

2. *For* $v \in [1, n]$, *calculate* $\sigma_v = lcm(g_i^{\S(v)})$ *(Theorem 3), and* $\sigma = \prod_{v=1}^{n} \sigma_v$

3. *Calculate* $\omega = \sigma\Gamma_{\tilde{e}}/\mathbf{X}$ *(Theorem 1)*

4. *By testing the values of* ω *and* σ, *find the error*

Applying Algorithm 1 to the code in previous Example will always correct all errors e for which Ξ_e is included in a rectangle with at two most two points per side. Algorithm 1 allows some errors of weight greater than half the minimum distance to be corrected, but does not a priori correct all errors with weight less than half the minimum distance.

An important criterion for the success of Algorithm 1 is the determination of $\Gamma_{\tilde{e}}$ from the known positions. In fact when we have recovered $\Gamma_{\tilde{e}}$ using σ, we can use the second remark at the end of Section 3 to compute $\omega = \iota(\sigma, \tilde{e})$. In the same way, *if we can write* $\Gamma_{\tilde{e}}(\mathbf{X^{-1}})$ *as*

$$\Gamma_{\tilde{e}}(\mathbf{X^{-1}}) = \frac{\mathbf{X}o(\mathbf{X})}{(1 - X_1^{N_1})(1 - X_2^{N_2})}$$

it suffices to remove common factors to obtain $\Gamma_{\tilde{e}}(\mathbf{X^{-1}}) = \dfrac{\mathbf{X}\omega(\mathbf{X})}{\sigma_1(X_1)\sigma_2(X_2)}$.

The Berlekamp Massey step can be computed in $O(\text{length}^2)$ operations, so if we restrict ourselves to such algorithms in step 1, Algorithm 1 admits a complexity of $\max_{v\in[1,n]} O(N_v^3)$. Moreover, notice that the search for $g_i^{\S(v)}$ can be performed simultaneously for each $v \in [1, n]$. So, Algorithm 1 seems to be practicable.

References

[1] Berman *" Semisimple cyclic and Abelian codes "* , *Cybernetics, Vol. 3, No. 3, pp. 17-23, 1967.*

[2] R. Blahut *" Theory and Practice of Error Control Codes "* , *Reading, MA : Addison-Wesley, 1983.*

[3] P. Camion *" Abelian codes "* *MRC Technical Summary Report No.1059, University of Wisconsin, Madison, Wisconsin, 1970.*

[4] J.L. Dornstetter *" On the equivalence between Berlekamp's and Euclid's algorithms "* , *IEEE Transactions on Information Theory, Vol. 33, pp. 428-431, 1987.*

[5] P. Fitzpatrick and G. H. Norton *" Linear recurrence relations and an extended sub-resultant algorithm "* , *Coding Theory and Applications , Springer Lecture Notes in Computer Science, Vol. 388, pp. 232-243, (Cohen G. and Wolfmann J. eds), 1989.*

[6] P. Fitzpatrick and G. H. Norton *" Finding a basis for the characteristic ideal of an n-dimensional linear recurring sequence "* , *IEEE Transactions on Information Theory, Vol. 36, pp. 1480-1487, 1990.*

[7] J. L. Massey, *" Shift Register synthesis and BCH decoding "* , *IEEE Transactions on Information Theory, Vol. IT-15, pp.122-127, Jan. 1969.*

[8] G. H. Norton *" On n-dimensional sequences, II. Characteristic Ideals "* , *submitted to J. Symbolic Computation, Feb. 1992.*

[9] P. Pedersen *" Calculating multidimensional symmetric functions using Jacobi's formula "* , *AAECC 9, New Orleans, Springer Lecture Notes in Computer Science, Vol. 539, pp. 304-317, LA, USA, (H.F. Mattson, T. Mora, T.R. Rao eds), 1991.*

[10] S. Sakata *" Decoding binary 2-D cyclic codes by the 2-D Berlekamp-Massey algorithm "* , *IEEE Transactions on Information Theory, Vol. 37, No.4, pp. 1200-1203, July. 1991.*

Acknowledgements

The first author wishes to thank Nicolas Sendrier and Daniel Augot for their help.
The second author gratefuly acknowledges support from SERC grant GR/H15141

ISSN 0249-6399